12.1. Обнаружение утечки конфиденциальной информации.

12.2. Сбой системы.

12.3. При попытке несанкционированного доступа к конфиденциальным данным.

Тот факт, что устройство на Android является мобильным, привносит новые проблемы, которых лишены стационарные компьютеры. В связи с этим имеют место разработки нового модуля DLP-системы. В данной работе сформулированы общие требования при разработке DLP-системы для мобильных устройств.

Библиографические ссылки

1. Википедия: свободная энциклопедия [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B5%D0%B4%D0%BE%D1%82%D0%B2%D1%80%D0%B0%D1%89%D0%B5%D0%BD%D0%B8%D0%B5_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8, свободный.

2. PCWEEK Безопасность [Электронный ресурс]. Режим доступа: http://www.pcweek.ru/security/article/detail.php?ID=109716, свободный.

3. Pointlane Информационная Безопасность [Электронный ресурс]. Режим доступа: http://www.pointlane.ru/solutions/dlp/, свободный.

4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21.

МЕТОД ОЦЕНКИ УЯЗВИМОСТЕЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АСУ ТП

А. И. Кураленко, А. С. Яценко
(Томск, ТУСУР, alkur@sibmail.com; yas@ttfoms.tomsk.ru)

Автоматизированные системы управления техническим процессом прочно вошли в нашу жизнь, на сегодняшний день они внедрены повсеместно, где необходима автоматизация. Для таких объек-

тов важнейшим требованием является надежность. Недопустимы их мелкие аварии и выход из строя даже на короткое время. Автоматизация управления объектами несет угрозу реализации деструктивного воздействия на информационно-телекоммуникационную инфраструктуру со стороны источников угроз. При проведении любых работ по автоматизации деятельности предприятий немаловажным и заслуживающим особого внимания является вопрос обеспечения информационной безопасности (ИБ) автоматизированных систем управления техническим процессом (АСУ ТП) [1]. Обеспечение информационной безопасности АСУ ТП достигается путем создания, эксплуатации, модернизации системы обеспечения безопасности информации (СОБИ). Это связанно с появлением новых уязвимостей, а как следствие – и новых угроз ИБ. При этом возникает необходимость определить возможные уязвимости, особенно при проектировании СОБИ, для того чтобы определить необходимые защитные меры, ведь от того, насколько СОБИ сможет противостоять угрозам ИБ, и будет складываться надежность АСУ ТП.

При обеспечении ИБ АСУ ТП основную опасность представляют преднамеренные действия источников угроз. Воздействие случайных факторов само не ведет к получению защищаемой информации, а лишь способствует появлению каналов получения информации, которыми может воспользоваться источник угрозы, злоумышленник [2]. Территориально деструктивные действия возможны в различных зонах, подробно о таких зонах сказано в [3].

При этом деструктивное действие в отношении информации может произойти при одновременном наступлении следующих событий:

– источник угрозы должен получить доступ в соответствующую зону;

– во время нахождения источника в зоне в ней должен иметь место канал получения информации;

– проявившийся канал должен быть доступен нарушителю соответствующей категории;

– в канале получения информации в момент доступа источника угроз должна находиться защищаемая информация.

Вероятность получения информации источником угрозы k-й категории по j-каналу в l-зоне i-го структурного компонента системы определяется следующей зависимостью:

$$P_{ijkl} = P_{ikl}^{(d)} P_{ijl}^{(k)} P_{ijkl}^{(n)} P_{ijl}^{(u)}, \quad (1)$$

где $P_{ikl}^{(d)}$ – вероятность доступа источника угрозы k-й категории в l-зоне i-го компонента системы; $P_{ijl}^{(k)}$ – вероятность проявления j-канала в l-зоне i-го компонента системы; $P_{ijkl}^{(n)}$ – вероятность доступа нарушителя k-й категории по j-каналу в l-зоне i-го компонента системы при условии доступа нарушителя в зону; $P_{ijl}^{(u)}$ – вероятность защищаемой информации в j-каналу в l-зоне в момент доступа туда нарушителя.

Вероятность получения информации в одном компоненте системы одним источником угроз одной категории по одному каналу назовем базовым показателем уязвимости информации. С учетом (1) выражение для базового показателя будет иметь вид:

$$P_{ijk}^{(6)} = 1 - \Pi_{m=1}^{5}(1 - P_{ijkl}) = 1 - \Pi_{m=1}^{5}(1 - P_{ikl}^{(d)} P_{ijl}^{(k)} P_{ijkl}^{(n)} P_{ijl}^{(u)}). \quad (2)$$

Рассчитанные таким образом базовые показатели уязвимости сами по себе имеют ограниченное практическое решение. Для решения задач, связанных с разработкой и эксплуатацией систем обеспечения безопасности информации, необходимы значения показателей уязвимости, обобщенные по какому-либо индексу (i, j, k) или по их комбинации.

Пусть $\{K^*\}$ – интересующее нас подмножество из полного множества потенциальных возможных нарушителей. Тогда вероятность нарушения защищаемой информации указанным подмножеством нарушителей по j-му фактору в i-м компоненте системы ($P_{\{K^*\}ij}$) определится

$$P_{\{K^*\}ij} = 1 - \Pi_{K^*}\left[1 - P_{ijk}^{(6)}\right], \quad (3)$$

где K^* означает перемножение в скобках для всех k, входящих в подмножество $\{K^*\}$.

Аналогично, если $\{J^*\}$ есть подмножество представляющих интерес каналов, то уязвимость информации в i-м компоненте по данному подмножеству факторов относительно k-го нарушителя определится

$$P_{\{J^*\}iK} = 1 - \Pi_{P_{\{I^*\}iK}} \left[1 - P_{ijk}^{(6)}\right]. \quad (4)$$

Наконец, есть $\{I^*\}$ есть подмножество интересующих нас структурных компонентов СОБИ, то уязвимость в них по j-му каналу относительно k-го нарушителя:

$$P_{\{I^*\}iK} = 1 - \Pi_{K^*} \left[1 - P_{ijk}^{(6)}\right]. \quad (5)$$

Каждое из приведенных выше выражений позволяет производить обобщение по какому-либо одному параметру. Нетрудно получить и общее выражение, если нас интересуют подмножества $\{I^*\}$, $\{J^*\}$ и $\{K^*\}$ одновременно. Общий показатель уязвимости P определяется выражением

$$P = 1 - \Pi_i \left[1 - P_{ijk}^{(6)}\right] \Pi_j \left[1 - P_{ijk}^{(6)}\right] \Pi_k \left[1 - P_{ijk}^{(6)}\right]. \quad (6)$$

Наибольший интерес представляют экстремальные показатели уязвимости, характеризующие неблагополучные условия защищенности: самый уязвимый компонент СОБИ, самый опасный канал съема информации, самая опасная категория нарушителя для данных условий [3].

Применение описанного метода затрудняется определением уязвимого компонента, потенциального канала съема, определением источника угроз. Существуют несколько способов избежать этих затруднений. Первый базируется на статистических данных о таких величинах. Но статистики по АСУ ТП в широком доступе нет на данный момент, поэтому этот подход практически неприменим. Следующий базируется на проведении работ экспертами [4]. Представителями экспертной комиссии определяются все значения коэффициентов, как следствия, вероятность уязвимости целиком зависит от работы экспертов.

Авторами данной работы предлагается вычисление оценки уязвимости по данному методу с использованием [5; 6]. В [5] содер-

жатся уже готовые статистические данные и инструментарий, позволяющий, зная данные об уязвимостях и их вероятностях, определить возможные и актуальные угрозы, в том числе с учетом перечня угроз, указанных в [6].

Библиографические ссылки

1. *Кирсанов С. В.* Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли //Докл. ТУСУР. 2013. № 2 (28). С. 115–118.

2. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов. М. : Горячая линия-Телеком, 2004. 280 с.

3. *Семкин С. Н., Беляков Э. В., Гребенев С. В., Козачок В. И.* Основы организационного обеспечения информационной безопасности объектов информатизации : учеб. пособие. М. : Гелиос АРВ, 2005. 192 с.

4. *Домарев В. В.* Безопасность информационных технологий. Системный подход. К. : ООО «ТИД ДС», 2004. 992 с.

5. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры : утв. зам. директора ФСТЭК России 18 мая 2007 г.

6. *Вихорев С. В.* Классификация угроз информационной безопасности. М. : ОАО «ЭЛВИС-ПЛЮС», 2001.

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ФАЙЛОВЫХ СИСТЕМАХ

Д. В. Куц
(Екатеринбург, УрФУ, Qcmail@rambler.ru)

Защита информации в файловых системах чрезвычайно важная и актуальная тема в области информационной безопасности.

Сбой файловой системы часто приносит не меньше проблем, чем отказ физического носителя. Восстановление информации оказывается делом трудным, длительным, а часто и невыполнимым. Очень многое в этом процессе зависит от используемой файловой системы. Поэтому вопросы надежности, защиты целостности фай-